The First U.S. Navy Cipher Machine? November 26

What was the Navy's first machine-generated cipher machine? Some naval cryptologic historians argue that it was the Naval Cipher Box, but an argument can also be made that it was the Communications Machine (CM),* invented in the early 1920s by Navy Lieutenant Commander William F. "Pop" Gresham. The CM was a mechanical cipher device based on a sliding alphabetic system. It was the first system that dispensed with a codebook. It became the standard navy cryptologic tool during the 1920s. Although it did require some hardware modifications later, it was essentially the Navy's first high-command cipher.

Herbert Yardley

CCH's intent in covering this invention is to showcase Army-Navy cryptologic cooperation during a time period when it was arguably non-existent. At the time, the Army's primary cryptologic unit was MI-8 (a.k.a. the Cipher Bureau), headed by Herbert O. Yardley, arguably America's pre-eminent cryptologist at the time. In fact, his influence was probably at its height, as his Cipher Bureau had just broken Japanese diplomatic codes that enabled the United States to out-negotiate the Japanese during the 1921-1922 Washington Naval Disarmament Conference.

The Navy, in comparison, had the Research Desk of its Code and Signal Section, headed by the abovementioned "Pop" Gresham. In July 1922, Gresham contacted Major Frank Moorman of the Army's Military Intelligence Division in Washington to request his opinion of Gresham's invention, enclosing samples of his encrypted messages along with the alphabets he designed for the device's use. Moorman simply forwarded the request to Yardley.

Yardley provided his evaluation of the Gresham machine in a July 21, 1922, note to Moorman. He admitted that he had not yet had time to read the messages enciphered by Gresham. However, based on their appearance and the accepted

codebreaking procedures of his day, he opined that the method of attack would essentially be the same as attacking a Bazeries Cylinder.** Yardley furthermore reasoned that since the rest of the world was already familiar with the Bazeries Cylinder (the U.S. Army also used it at the time), Gresham's new machine would logically be breakable by an adversary.

Could Yardley make Gresham's device better? He told Moorman that "if Commander Gresham is really desirous of learning the strengths and weaknesses of his cipher, I would think that he should be willing to turn his machine over to us." He offered to educate Gresham further about the Bazeries Cylinder, to include what his Cipher Bureau would do to protect codes during wartime. Yet he offered no guarantees of total invincibility for Gresham's cipher. Yardley did acknowledge though that the Bazeries Cylinder provided security for a while because codebreaking was not a fast process.

Finally, Yardley, then New York City-based, offered to discuss the Gresham cipher in person with both Moorman and Gresham when he traveled to Washington, D.C. in early August. CCH, for the record, does not yet know if the meeting was ever held. CCH does presume though that the Gresham cipher evaluated by Yardley, because of the time line involved, was probably Gresham's eventual CM invention.

As a historical note, the CM had a more well-known co-founder. When Gresham died in 1935, his widow made a claim for recompense. As Congress investigated the claim, Agnes Meyer Driscoll, the Navy's principal civilian cryptanalyst for many years and Gresham's underling at the time, claimed a share in the invention. She was successful to the point that both she and Mrs. Gresham received money for the invention in 1937.

* It was later known just as the "Cipher Machine"

** Named after the French military cryptologist Étienne Bazeries, the Bazeries Cylinder is essentially an improved version of the (Thomas) Jefferson Disk or wheel cipher, currently on display at the National Cryptologic Museum. Yardley, by the way, consistently dropped the "s" (Bazerie) in his correspondence with Moorman.

The Jefferson Cipher, on which the Bazeries cipher was modeled

Sources: “Madame X: Agnes Meyer Driscoll and U.S. Naval Cryptology, 1919-1940,”

Cryptologic Almanac 50th Anniversary Series, DOCID: 3575740 (available on NSA unclassified website);

CCH internal source records, e.g., AMD References in Holtwick's Naval Security Group History of World War II, SRH-355, Part 1;

Background information on Yardley, early Navy cryptologic organizations, and ciphers, Bazeries Cylinder and Jefferson Disk

508 caption: photo 1, head shot of a balding Herbert Yardley; photo 2, the Jefferson cipher device, brown disks on a spindle, displayed on a cloth of deep blue.